

KONDRA

SIEM, MDR, CTI POUR LES PME



KONDRA :

UNE SURVEILLANCE JOUR ET NUIT, SANS MONTER VOTRE PROPRE SOC.

Vos pare-feu, vos postes Windows et votre tenant Microsoft 365 consignent déjà ce qui se passe sur le réseau. Mais presque personne ne lit ces journaux. Les surveiller en continu exige un centre des opérations de sécurité (SOC) avec des analystes qui se relaient, ce que peu de PME peuvent se permettre.

Les journaux s'accumulent, et on ne découvre généralement une intrusion qu'une fois les dégâts constatés.

Kondra collecte ces journaux, les indexe dès leur arrivée et analyse en plus le trafic réseau via un port miroir de votre switch. Des règles de détection et le renseignement sur les menaces en extraient des alertes, que les analystes d'EXYS traitent 24 heures sur 24.

Tout fonctionne sur un boîtier installé dans votre propre réseau. Les analystes consultent vos données sur place : elles ne quittent jamais vos locaux.

LA SÉCURITÉ D'UN GRAND GROUPE.
LE BUDGET D'UNE PME.

Le boîtier écoute le trafic de façon passive sur un port miroir et analyse plus de 20 protocoles réseau. Connexions inhabituelles, hôtes mal configurés et fuites de données ressortent, même sur des machines où rien n'est installé.

Ombra, l'agent de Kondra pour les postes, complète ce que le réseau ne voit pas : les applications installées et la configuration de chaque machine. Les modifications d'utilisateurs, de groupes et de stratégies de groupe dans Active Directory sont aussi enregistrées : la création d'un compte administrateur peut ainsi déclencher une alerte.

Après chaque incident, auditeurs et autorités de surveillance posent les mêmes questions : ce qui s'est passé, quand, et ce qui a été fait. Avec Kondra, les réponses sont déjà consignées. Chaque événement est consultable, le SOC d'EXYS ouvre un dossier avec les journaux et les indicateurs de compromission (IoC), et le rapport forensique est rédigé à partir des mêmes données. La durée de conservation est fixée par client, selon ce qu'exigent vos auditeurs, les autorités ou vos règles internes. EXYS est elle-même certifiée ISO 27001.



CE QUI EST INCLUS :

- Boîtier sur site dimensionné selon votre nombre de postes, les journaux restent chez vous
- Surveillance et réponse 24/7 par les analystes du SOC d'EXYS
- Surveillance réseau passive sur un port miroir, plus de 20 protocoles
- Journaux de pare-feu de différents fabricants, de Microsoft 365, des événements Windows, du réseau et des IDS, plus d'autres sources sur demande
- Corrélation avec du renseignement sur les menaces open source et propriétaire
- Tableaux de bord prêts à l'emploi, carte réseau des hôtes à problème et alertes multicanal
- Agent de poste Ombra pour l'inventaire logiciel et la configuration des postes
- Suivi des modifications Active Directory : utilisateurs, groupes, stratégies de groupe et unités d'organisation
- Gestion des incidents au sein du SOC d'EXYS, avec journaux, IoC et rapports forensiques liés
- Matrices MITRE ATT&CK et RE&CT montrant la couverture de détection et de réponse
- Analyse de logiciels malveillants, avec fichiers isolés et captures PCAP conservés pour l'enquête
- Extensions pour la gestion des événements OT
- Conservation des journaux, contrôles d'intégrité et sauvegarde pour les audits de conformité

CONTACTEZ-NOUS

ADRESSE

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Suisse

CONTACT

Tél. +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA est certifiée ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY
EXYS7950 - KONDRA